Додаток Б

Презентація

Методи виявлення та нейтралізації загроз для безпеки даних у системах електронної комерції

Здобувач: Хімченко О. С. ІСТм-24
Керівник: д.т.н., професор Бородавка Є. В.

ВСТУП

Розвиток інформаційних технологій та цифровізація економіки сприяли стрімкому зростанню електронної комерції, яка стала невід'ємною частиною повсякденного життя мільйонів користувачів.

Разом з розширенням електронної комерції, експоненціально зростають масштаби та складність загроз інформаційній безпеці. Системи е-комерції обробляють й акумулюють величезні обсяги критично важливих даних: персональну інформацію користувачів, платіжні реквізити, комерційні таємниці та історії транзакцій. Така концентрація чутливої інформації робить ці платформи привабливою мішенню для кіберзлочинців, хакерів та інших загроз.

На сьогодні продовжується постійне зростання кількості успішних кібератак на системи електронної комерції, що призводять до витоків даних, фінансових збитків для компаній та втрати довіри споживачів до цифрових каналів торгівлі.

3

Аналіз предметної області та постановка задачі

Предметною областю цієї роботи є **електронна комерція** (e-commerce) – галузь економіки, в якій реклама, просування продуктів, торговельні угоди та фінансові транзакції здійснюються безпосередньо в Інтернеті. Коли ви щось купуєте чи продаєте у мережі, це і є e-commerce.

E-commerce розділяють на шість основних видів залежно від взаємодії сторін: клієнтів, бізнесу та адміністрацій. Видами та типами електронної комерції є:

- **B2B** – електронна комерція для бізнесу. Це різновид електронної комерції, який працює за принципом "від бізнесу - бізнесу" (Business-to-Business);

4

Аналіз предметної області та постановка задачі

- **B2C** – електронна комерція для споживача. Наразі модель Business-to-Consumer (B2C) – це найпоширеніший вид електронної комерції;
- **C2C** – електронна комерція між споживачами. Це модель електронної комерції, в межах якої один споживач продає щось іншим споживачам, маючи з ними рівний статус (Consumer-to-Consumer);
- **C2B** – електронна комерція від споживача до бізнесу. Це фактично пряма протилежність B2C, оскільки в цьому випадку вже споживач надає певні товари та послуги бізнесу (Consumer-to-Business);
- **B2A** – бізнес-адміністрування. Модель B2A (Business-to-Administration) або B2G (Business-to-Government) подібна B2B;
- **C2A** – електронна комерція між споживачами та адміністрацією (Consumer-to-Administration).

5

Аналіз предметної області та постановка задачі

Мета роботи полягає у розробці та обґрунтуванні комплексу методів виявлення та нейтралізації загроз для безпеки даних у системах електронної комерції для автоматизації та спрощення оцінки стану безпеки, а також забезпечення швидкого та своєчасного реагування на виявлені загрози.

Об'єктом дослідження є дані у системах е-комерції, загрози безпеці та процеси їх виявлення та нейтралізації, що охоплюють автентифікацію користувачів, управління доступом, моніторинг операцій та реагування на інциденти.

Предметом дослідження є методи та алгоритми виявлення загроз, модельні підходи до класифікації атак та аномалій, а також механізми криптографічного захисту даних та управління аутентифікацією в e-commerce системах.

6

Види даних та вимоги до безпеки

Які є **види даних** в системах електронної комерції:

- Персональні дані користувача
- Платіжні та фінансові дані
- Комерційні дані та бізнес-логіка
- Системні логи та журнали аудиту

Вимоги до інформаційної безпеки складає традиційна **тріада CIA** (Confidentiality, Integrity, Availability) але є недостатнім базисом для сучасних систем електронної комерції. Тому вона вимагає розширення ще двома додатковими елементами: Автентичністю (Authenticity) та Невідмовністю (Non-repudiation).

7

Класифікація загроз та методи їх виявлення

У контексті даної роботи було виділено такі основні **групи загроз**:

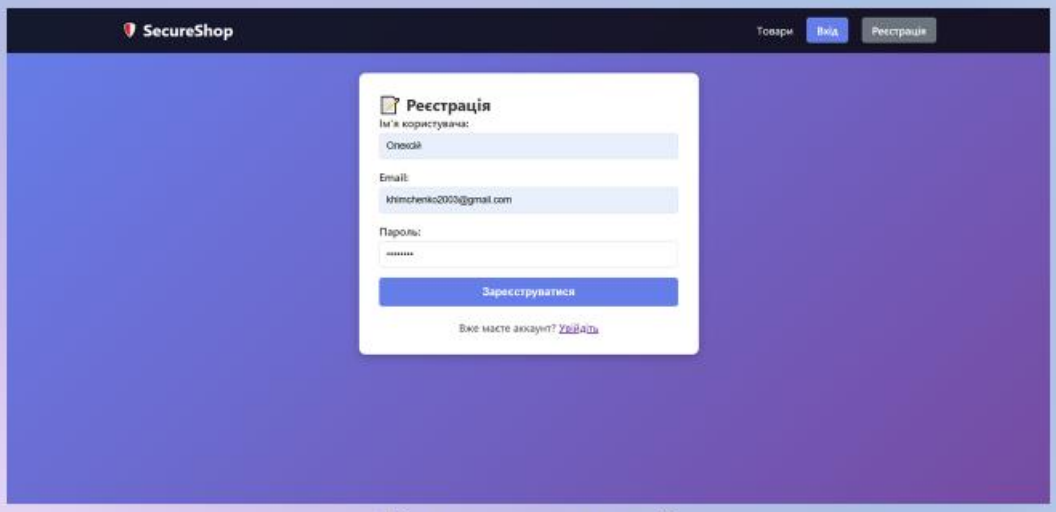
- атаки на веб-додаток;
- атаки на мережевій інфраструктурі;
- атаки на облікові записи користувачів;
- загрози, пов'язані з платіжними операціями;
- загрози на основі соціальної інженерії та внутрішніх зловживань.

Методи виявлення загроз у системах електронної комерції можна поділити на такі групи:

- сигнатурні (правилові) методи;
- методи аномалійної детекції;
- методи машинного та глибинного навчання;
- поведінковий аналіз;
- контекстний та кореляційний аналіз подій.

8

Практична реалізація



Процес реєстрації

Збереження даних користувача

9

Після успішної реєстрації, в базі даних з'являється запис про нового користувача. Як можна помітити, збережений пароль є зашифрованим

	id	username	email	password_hash	role	created_at
1	1	admin	admin@shop.com	e935887960d78ac38fd67cf1c4a6aa8c71376c81dd1c546e2793ef919fd2e2c48b5b2a241f0ef48f130b01fef7982065b295a1fb85b4ec6afa6	admin	2025-12-06 21:24:04.486003
2	2	Олексій	khimchenko2003@gmail.com	scrypt:...	user	2025-12-06 21:27:54.667503

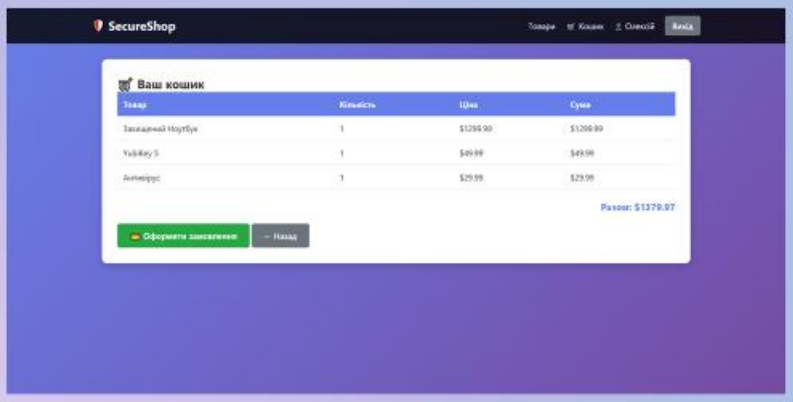
Для шифрування використовується бібліотека werkzeug мови програмування python

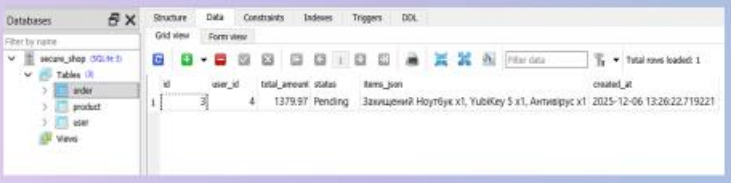
```
@app.route( rule: '/register', methods=['GET', 'POST']) 3 usages
def register():
    if request.method == 'POST':
        username = request.form.get('username', '').strip()
        email = request.form.get('email', '').strip()
        password = request.form.get('password', '')
```

```
user = User(username=username, email=email, password_hash=generate_password_hash(password))
db.session.add(user)
```

Процес замовлення товару і додавання до БД

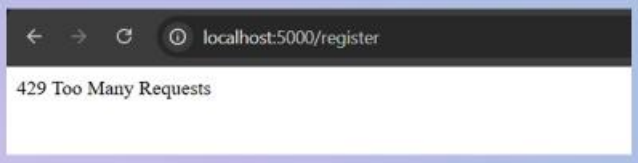
10





11

Перевірка безпеки



Після надсилання великої кількості запитів, система сприймає це як загрозу і блокує IP адресу, з якої була підозріла активність і надсилається попередження про блокування IP адреси.

12

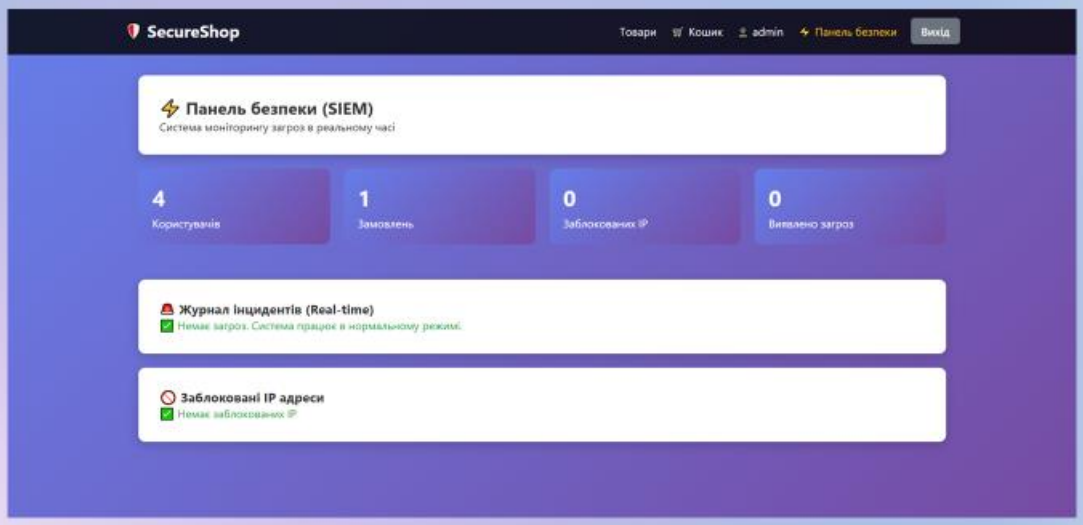
Реалізація безпеки від DDoS атаки

```python
now = time.time()
if ip not in threat_engine.request_history:
    threat_engine.request_history[ip] = []

threat_engine.request_history[ip] = [t for t in threat_engine.request_history[ip] if now - t < 10]
threat_engine.request_history[ip].append(now)

if len(threat_engine.request_history[ip]) > 30:
    threat_engine.block_ip(ip)
    threat_engine.log_incident(ip, attack_type: "DDoS Attack", payload: "Too many requests")
    return "429 Too Many Requests", 429
```

Захист від DDoS атак (надмірної кількості запитів) реалізується за допомогою перевірки кількості запитів, де запити старіше 10 секунд видаляються, а якщо кількість запитів перевищує 30, тоді IP потрапляє до чорного списку.

13

Панель безпеки адміна



14

Висновок

Під час виконання роботи було досліджено види даних в електронній безпеці та вимоги до їхньої безпеки. Було розглянуто класифікацію загроз і методи їх виявлення.

Після теоретичного аналізу було спроєктовано архітектуру системи і виконання програмної реалізації захищеної системи, яка враховує вимоги інформаційної безпеки.

Проведено тестування розробленої системи, під час якого відбулась перевірка хешування паролів користувачів і змодельовано DDoS атаку, яка була успішно виявлена та знешкоджена.